Amendments to the Specification:

Please replace the paragraph beginning on page 8, line 10 with the following paragraph. Support for the amendments to this paragraph can be found in the paragraph as originally submitted; in Figure 1 as originally submitted; in page 13, lines 6-14; and page 13, line 24 through page 14, line 26.

> FIG. 1 shows a pictorial representation of an environment (100) in which a preferred embodiment of the present invention may be implemented. There is shown multiple users (105), each having access to a shared device (110) (e.g. a personal computer, a personal digital assistant (PDA) etc.). Shared device (110) communicates with server (120) via network (115).

Please replace the paragraph beginning on page 8, line 19 with the following paragraph. Support for the amendments to this paragraph can be found in Figure 2 as originally filed; in Figure 1 as originally filed, and in the specification on page 8, line 11 through page 9, line 9.

> Referring to FIG. 2 and FIG. 4, there is shown an overview of an environment (230) wherein a user (105) has access to a device (110), the device comprising stored data. Preferably, a user presents (step 400) a token (200) (e.g. a SmartCard) to the device (110). Preferably, a user identity authentication means is stored on the SmartCard (200), for example a key. In one embodiment, a user enters some personal data (e.g. a Personal Identification Number (PIN)) after the SmartCard (200) is presented to the shared device (110) and a hashing algorithm is applied to the PIN in order to dynamically generate a key on the SmartCard (200) itself. However in a more advanced system the key may be generated from biometric data read by a reader adapted to recognise particular facial or other characteristics of the user such as fingerprint or hand geometry. In an alternative embodiment, an authentication key is pre-generated and stored on the SmartCard (200). In yet another embodiment, the user identity authentication means is a digital certificate comprising a key and a user id.

Please replace the paragraph beginning on page 14, line 11 with the following paragraph. Support for the amendments to this paragraph can be found in the paragraph as originally submitted.

> Those skilled in the art will appreciate that such computer readable instructions can be written in a number of programming languages for use with many computer architectures or operating systems. Further, such instructions may be stored using any memory technology, ~~present or future,~~ including but not limited

to, semiconductor, magnetic, or optical, or transmitted using any communications technology, ~~present or future,~~ including but not limited to optical, infrared, or microwave. It is contemplated that such a computer program product may be distributed as a removable media with accompanying printed or electronic documentation, e.g., shrink wrapped software, pre-loaded with a computer system, e.g., on a system ROM or fixed disk, or distributed from a server or electronic bulletin board over a network, e.g., the Internet or World Wide Web.

Please add the following new paragraph just before the paragraph beginning on page 13, line 24 and just after the paragraph ending on page 13, line 23. Support for this new paragraph can be found in the abstract as originally filed, as this paragraph duplicates the abstract as originally filed.

A data processing system for controlling access of at least one user to stored data is provided. The system comprises means, responsive to a request from the user to access a set of the stored data, for authenticating the user. The system also comprises means, responsive to successful authentication, for decrypting an encrypted data structure associated with the user. The data structure comprises data associated with the set (e.g. location of the set). The system also comprises means, responsive to successful decryption, for accessing the set.